RBI Digital Payment Security Directions, 2026

Prelims: Current events of National and International Importance | Economy

Why is in news?

The Reserve Bank of India (RBI) issued the ***Digital Payment Security Controls Directions, 2026*** for commercial banks on July 31, 2026. It also consolidated cyber-resilience and digital-payment security requirements for authorized non-bank Payment System Operators (PSOs) through Master Directions issued on November 5, 2026.

About the Directions

- The commercial-bank directions apply to digital payment products and services, including fund transfers, balance enquiry, PIN setting or changing, mobile banking registration, OTP generation, mini-statements, transaction-status checks and grievance facilities.
- They cover services offered directly by banks or through RBI-operated systems and ***RBI-authorised Payment System Operators***, along with the associated applications, systems and IT infrastructure.
- The directions apply to commercial banks, including SBI and corresponding new banks; Small Finance Banks, Payments Banks and Local Area Banks are outside this particular commercial-bank direction and are governed by separate directions.
- The framework seeks to strengthen confidentiality, integrity and availability of digital-payment systems while improving customer protection and resilience against cyber threats.

Key security requirements

- Board-approved policy: Banks must have a policy for digital payment products and services, reviewed at least annually, with the Board and senior management responsible for implementation.
- ***Multi-factor authentication (MFA)***: Banks must use MFA for electronic payments and fund transfers, except where specifically permitted or relaxed. At least one factor must be dynamic or non-replicable, such as OTP, device binding, biometrics or suitable hardware-based authentication.
- Transaction alerts: Alerts and MFA are required for payment transactions, addition/modification/deletion of beneficiaries, changes in account details and revisions to fund-transfer limits. Merchant name should be identified in OTPs/alerts wherever applicable.
- Fraud-risk monitoring: Banks must monitor suspicious patterns such as unusually rapid transfers, high-risk merchant activity, abnormal geo-location/IP patterns, behavioural indicators and transactions linked to reported fraud.
- Reconciliation: A real-time or near-real-time reconciliation framework must be established with relevant payment ecosystem participants; reconciliation should not be later than 24 hours from receipt of settlement files.
- Customer protection: Apps must provide secure-usage guidance, accessible grievance-

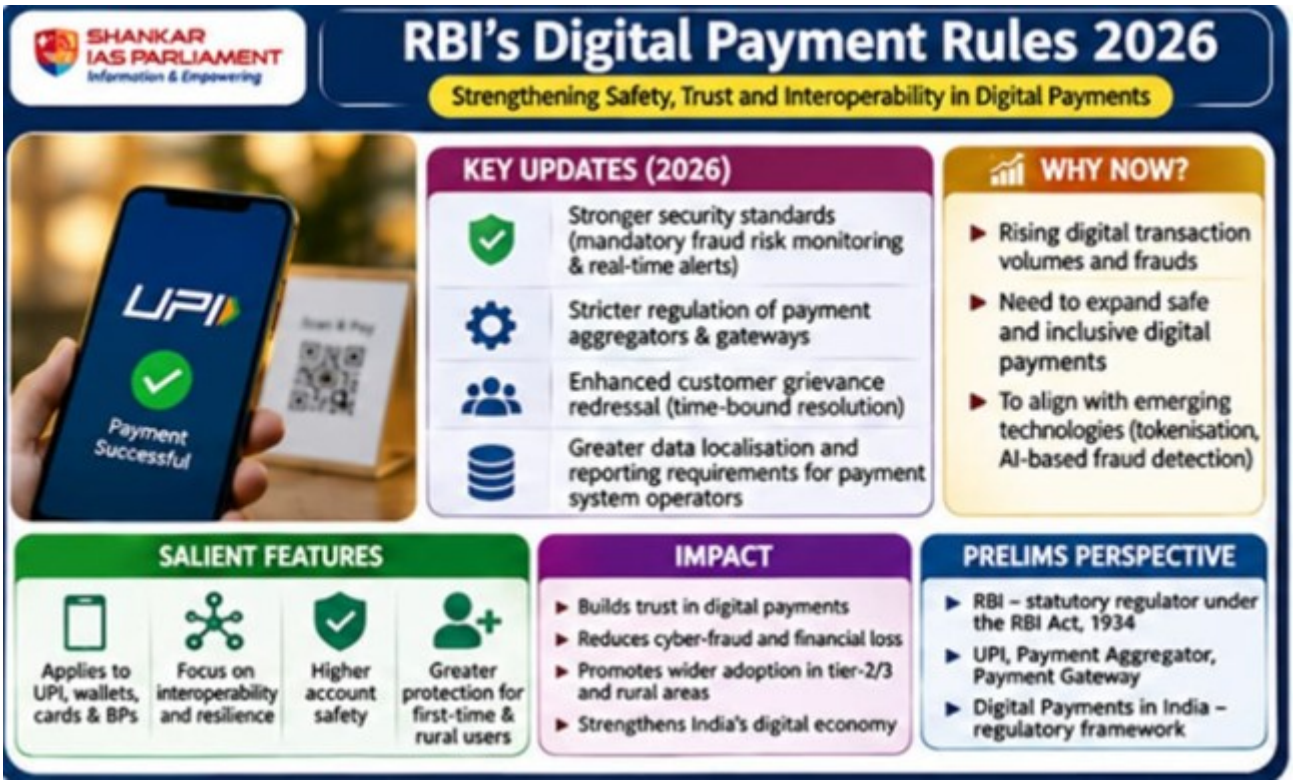
registration facilities and clear dispute-resolution procedures. Customers should be warned about phishing, vishing and remote-access scams.
- System resilience: Banks must assess technology and third-party risks, test applications and maintain backup and recovery arrangements to reduce service disruption.

Master Directions for non-bank PSOs

- The November 5, 2026 Master Directions consolidate requirements relating to cyber resilience and digital-payment security for authorised non-bank PSOs.
- They cover risks arising from ***connections with third-party service providers***, payment gateways, vendors and other entities in the digital-payment ecosystem.
- The directions take effect upon publication for large and medium non-bank PSOs; small non-bank PSOs are required to comply from April 1, 2028.

Legal and institutional framework

- The commercial-bank directions draw authority from the ***Banking Regulation Act, 1949 and the Payment and Settlement Systems Act, 2007***.
- The November 2026 directions for non-bank PSOs are issued under Section 10(2) read with Section 18 of the Payment and Settlement Systems Act, 2007.



Reference

RBI | Digital Payment Security Controls Directions, 2026

SHANKAR IAS PARLIAMENT
Information is Empowering